SUBSTITUTE ABSTRACT OF THE DISCLOSURE

The disclosed technology of the present invention relates to an information processing device such as an IC card, and specifically to the overflow processing which occurs in a modular multiplication operation during crypto-processing. Such overflow processing exhibits a particular pattern of consumption current. It is the subject of the present invention to decrease the relationship between the data processing and the pattern of the consumption current. In the processing procedures for performing a modular exponentiation operation according to the 2 bit addition chain method, the modular multiplication operation to be executed is selected at random, the selected modular multiplication operation is executed for each 2 bits, the correction of the result is performed, and the result of the calculation (i.e, a corrected value or uncorrected value) is outputted.